

Collection with PowerUpSQL



Ricardo Reimao

CYBER SECURITY CONSULTANT



Target: Microsoft SQL Server

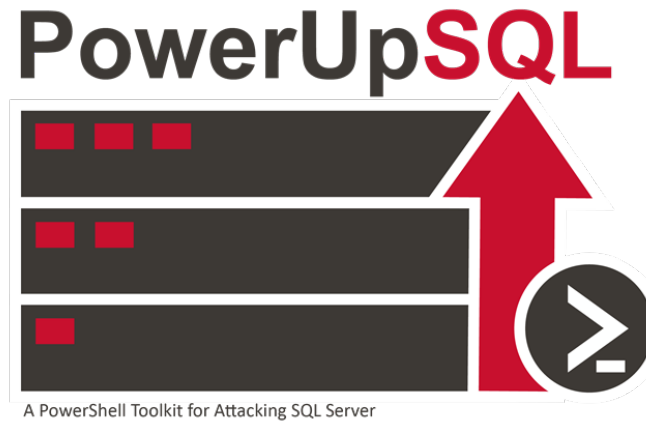


PowerUpSQL



A PowerShell Toolkit for Attacking SQL Server

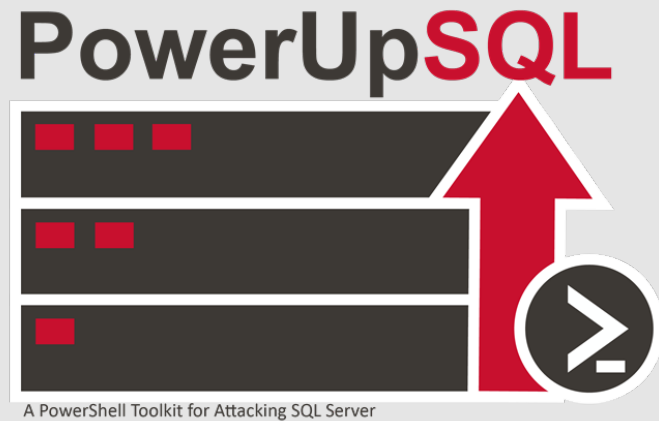




Author: Scott Sutherland
@_nullbind

PowerUpSQL includes functions that support SQL Server discovery, weak configuration auditing, privilege escalation on scale, and post exploitation actions such as OS command execution.





Open source tool

<https://github.com/NetSPI/PowerUpSQL>

Full framework for MS SQL auditing

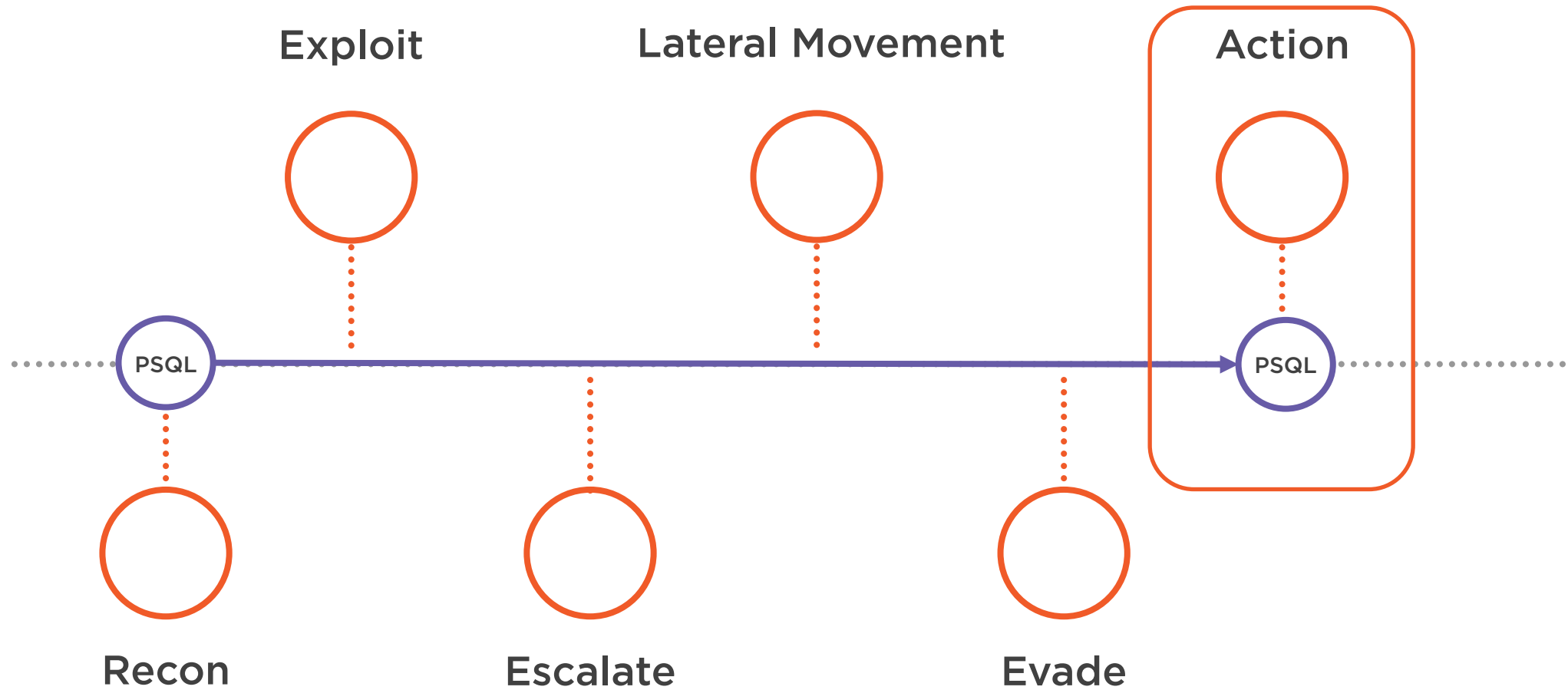
- Reconnaissance, initial access, privilege escalation, collection, etc.

Automate collection of sensitive data

- Find sensitive data
- Find credit card information
- Dump databases



Kill Chain



MITRE ATT&CK

Tactics

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command & Control
Exfiltration
Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1078:

Valid Accounts



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1005:

Data From Local System



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1485:

Data Destruction

T1565.001:

Stored Data Manipulation



Staying Legal

Stealing data without authorization is **ILLEGAL** in most countries



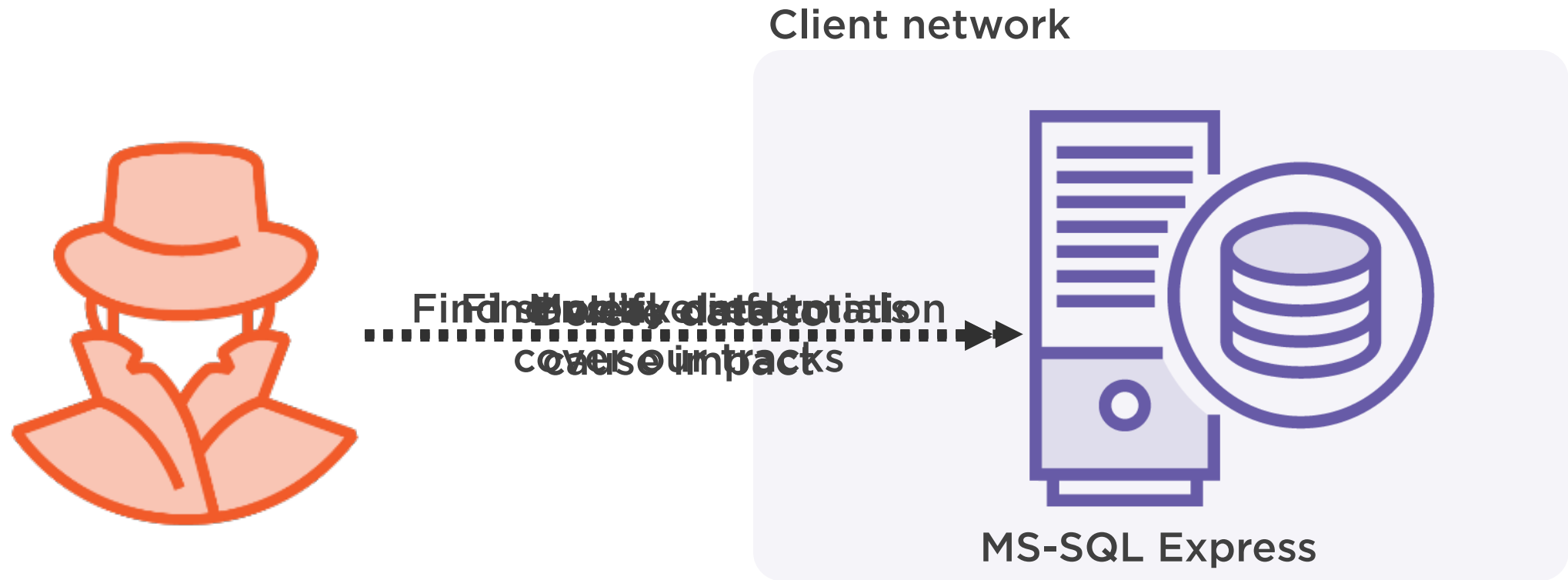
Letter of engagement, detailing dates and scope of what will be executed

Formal document, signed by the client, authorizing the types of attack you may perform

Always consult the client before any attack that may impact the network



Attack Explanation



Prerequisites



Attacker Machine

Windows 10 with Powershell
Or
Kali Linux



Target Machine

Microsoft SQL Express
or
Microsoft SQL Enterprise



Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



Other PowerUpSQL Features

Discovery

**Initial
Access**

**Insecure
Configurations**

**Privilege
Escalation**

Persistence

Exfiltration

<https://github.com/NetSPI/PowerUpSQL/wiki/PowerUpSQL-Cheat-Sheet>



More Information

Official Documentation

Several other capabilities
<https://github.com/NetSPI/PowerUpSQL/wiki>

Author Talk

BlackHat 2018
https://www.youtube.com/watch?v=UX_tBJQtqW0

Collection

Collection with PowerSploit
<https://pluralsight.com/library/courses/collection-powersploit/>

Remediation

Audit your own company

Do not reuse accounts

Strong passwords

Secure configuration



Thank you!



Ricardo Reimao
Cyber security consultant

